NICHOLAS A. CARLIN (State Bar No. 112532)
BRIAN S. CONLON (State Bar No. 303456)
PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 - The Presidio
San Francisco, CA 94129
Telephone: 415-398-0900
Fax: 415-398-0911
Email: nac@phillaw.com
bsc@phillaw.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JONATHAN D. RUBIN, individually and on behalf of all those similarly situated,

Plaintiffs,

v.

FACEBOOK, INC, a Delaware corporation; SCL GROUP, a United Kingdom company; GLOBAL SCIENCE RESEARCH LTD, a United Kingdom company; and CAMBRIDGE ANALYTICA LLC, a Delaware limited liability company.

Defendants.

Case No:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

SUMMARY OF THE CASE

1. On March 17, 2018, Christopher Wylie, a whistleblower and co-founder of Defendant CAMBRIDGE ANALYTICA LLC, revealed that his firm, under the direction of its Vice President and Secretary, Stephen Kevin Bannon, had used sensitive and personal information of over 50 million Americans harvested illegally via defendant FACEBOOK to manipulate American elections. The breach began in 2014, but FACEBOOK has still yet to notify its users of the breach in plain violation of California law.

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

2. Plaintiff JONATHAN D. RUBIN brings this lawsuit against Defendants individually and on behalf of a class including all other similarly situated users of FACEBOOK.

PARTIES

3. Plaintiff Jonathan D. Rubin is a resident of Los Angeles, California and an individual user of FACEBOOK during the relevant time period.

4. On information and belief, Defendant SCL (Strategic Communication Laboratories) GROUP ("SCL") is a private British behavioral research and strategic communications company which owns and operates Defendant CAMBRIDGE ANALYTICA LLC. On information and belief, SCL does significant business in California.

5. On information and belief, Defendant CAMBRIDGE ANALYTICA LLC ("CAMBRIDGE") is a Delaware limited liability company owned and operated by SCL, involved in data mining and data analysis. The company maintains offices in New York and Washington D.C. and does significant business in California. Steven Kevin Bannon ("Bannon") was Vice President and Secretary of CAMBRIDGE until he stepped down from that position to run Donald Trump's presidential campaign. On information and belief, Bannon had decision-making authority at CAMBRIDGE and directed and approved every action taken by CAMBRIDGE as alleged herein.

6. On information and belief, Defendant GLOBAL SCIENCE RESEARCH LTD. ("GSR") was a United Kingdom company which harvested and sold the private information of social media users for profit. On information and belief, GSR did significant business in California, but has since dissolved and its successors in interest are unknown at this time.

7. On information and belief, defendant FACEBOOK, INC. ("FACEBOOK") is a Delaware corporation with its principal place of business and main operations hub located in Menlo Park, California. FACEBOOK is an omni-present social media company, whose website was launched in 2004 and that now has more than two billion active users.

8. Unless separately identified, SCL, CAMBRIDGE, and GSR will be referred to herein as the "Co-Conspirators."The business association among and between the Co-Conspirators will be referred to herein as the "Political Deceit and Manipulation Enterprise."

9. Unless separately identified, SCL, CAMBRIDGE, GSR, and FACEBOOK will be referred to herein as the "Defendants."

JURISDICTION AND VENUE

10. This Court has original subject matter jurisdiction over this action pursuant to 18 U.S.C. § 1964. The Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

11. This Court has original jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because (a) at least one member of the putative class is a citizen of a state different from Defendants, (b) the amount in controversy exceeds $5,000,000, exclusive of interest and costs, (c) the proposed class consists of more than 100 class members, and (d) none of the exceptions under the subsection apply to this action.

12. This Court has jurisdiction over Defendants because they conduct business in California, both in connection with the facts giving rise to this lawsuit and during the general course of their affairs, and have sufficient minimum contacts in California, or otherwise intentionally avail themselves of the markets within California, through the promotion, sale, marketing and distribution of their services and products in California, to render the exercise of jurisdiction by this Court proper and necessary.

13. Venue is proper in this District under 28 U.S.C. § 1391 and 18 U.S.C. § 1965 because a substantial part of the events giving rise to Plaintiff's claims occurred within this District.

COMMON FACTUAL ALLEGATIONS

14. FACEBOOK is an onmi-present social media company which allows billions of people, and hundreds of millions of Americans, to connect through its platform. As part of its services, FACEBOOK asks its users for a plethora of private information, including biographical information, birthday, family and relationship status, what the user is interested in, their religious and political views, their websites, whether they are online at any given time, posts to the user's timeline or those of their friends, their hometown, their current location, their

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

education and work history, their activities, interests, posts and pages they liked, and their activity in different FACEBOOK-connected apps ("User Information"). Importantly, users control – or at least are led to believe they control – with whom they share User Information, whether it be privately with one or more individuals, to all their friends, their friends of friends, or the public at large. Users reasonably expect User Information will only be accessible to the types of people they allow to see it.

15. On March 17, 2018, the Guardian reported, based on information provided by Christopher Wylie, a co-founder of CAMBRIDGE, that dating back to at least 2014, Defendants SCL,CAMBRIDGE and GSR obtained from FACEBOOK the private information of at least 50 million American FACEBOOK users who did not consent to their information being shared with SCL, CAMBRIDGE, or any other related companies or individuals.

16. In June 2014, SCL entered into a written agreement with GSR. The agreement provided that GSR would harvest and process Facebook data so that SCL and its American subsidiary, CAMBRIDGE, could analyze it and use it to manipulate the American public in upcoming elections, including the 2016 presidential election. On information and belief, SCL would not have entered into this agreement with GSR without CAMBRIDGE's direction and approval, which it gave.

17. On information and belief, CAMBRIDGE and SCL spent $7 million to amass the data it acquired, and paid about $1 million to GSR alone.

18. On information and belief, these payments were made through wire transfer or other electronic payment method.

19. On information and belief, GSR, at the direction and with the kull knowledge of SCL and CAMBRIDGE, created a fake online personality quiz and paid a nominal fee to take it. GSR solicited participants through Amazon's Mechanical Turk and Qualtrics' markets. To take the quiz, users had to use GSR's app, "thisismydigitallife."This app enabled GSR to access the FACEBOOK profile of the person who took the quiz *and the profiles and private information of all their FACEBOOK friends.*

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

20. On information and belief, CAMBRIDGE wrote the terms of service for the app, and provided the legal advice guiding its creation.

21. On information and belief, the terms of service of GRS's app falsely represented to users that it was collecting information for academic purposes.

22. On information and belief, the nominal fees paid to quiz participants were made via transfer or other electronic means via the internet.

23. The result was that around 320,000 FACEBOOK users took these fake quizzes, resulting in 50 million people having their private User Information harvested for use by SCL and CAMBRIDGE, without their consent. These entities and individuals later used the data to manipulate and attempt to manipulate the voting of the American public.

24. On information and belief, FACEBOOK knew or should have known of GSR, SCL, and CAMBRIDGE's illegal scheme to obtain the User Information of its users in 2014 when it was happening, but did nothing to stop it.

25. Sandy Paraklias, a former Facebook operations manager responsible for policing data breaches by third-party software developers in 2011 and 2012, has stated that FACEBOOK was aware of the problem of third-party apps obtaining information from FACEBOOK users who had not authorized the apps themselves, but were relying on terms of service and settings that people didn't read or understand, instead of fixing the problem. See *https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas*.

26. Paraklias stated that GSR's app was "one of the very last to have access to friend permissions," meaning that FACEBOOK was well-aware of the problem by the time GSR, SCL and CAMBRIDGE used it to acquire User Information of 50 million FACEBOOK users without their permission.

27. It was not until August 2016 when FACEBOOK wrote a letter to Wylie, stating that the data must be deleted immediately, that FACEBOOK did anything to address GSR, SCL, and CAMBRIDGE's data theft. But this was two years after the data was harvested, and had already been used and weaponized against the American public by SCL and CAMBRIDGE at

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

Bannon's direction. Deleting the data at that point was meaningless; indeed, Wylie stated that he had already deleted the data by that point and that FACEBOOK made "zero effort to get the data back."

28. FACEBOOK never notified the 50 million users that their User Information had been compromised.

FACEBOOK's Security Practices are Inadequate and Their Representations to Their Users are Misleading

29. Despite growing efforts by hackers and others to illegally access personal information maintained by social media companies and the emphasis on data security in social media companies, FACEBOOK (1) failed to implement security measures and technological safeguards designed to prevent this type of attack even though social media is particularly vulnerable to this type of data theft; (2) failed to employ security protocols to detect the unauthorized network activity (or if it did, to sufficiently act on the breach), and (3) failed to maintain basic security measures.

30. This despite FACEBOOK stating publicly that "Protecting people's information is at the heart of everything we do." See *https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.*

31. On March 19, 2018, *Bloomberg* published an article entitled "FTC Probing Facebook For Use of Personal Data, Source Says," disclosing that the U.S. Federal Trade Commission ("FTC") was "probing whether Facebook violated terms of a 2011 consent decree of its handling of user data that was transferred to [CAMBRIDGE] without [user] knowledge." Under the 2011 settlement with the FTC, FACEBOOK "agreed to get user consent for certain changes to privacy settings as part of a settlement of federal charges that it deceived consumers and forced them to share more Personal Information than they intended." The article further stated that "if the FTC finds Facebook violated terms of the consent decree, it has the power to fine the company more than $40,000 a day per violation."

32. At all relevant times, FACEBOOK has maintained a Data Use Policy on its website, which advised FACEBOOK users, in part: "While you are allowing us to use the

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

information we receive about you, **you always own all of your information. Your trust is important to us, which is why we don't share information we receive about you with others unless we have: [1] received your permission; [2] given you notice,** such as by telling you about in this policy; or [3] removed your name and any other personally identifying information from it." https://www.facebook.com/full_data_use_policy (emphasis added).

33. On information and belief, none of the friends of the individuals who took GSR's quiz gave FACEBOOK permission to share their personal and private User Information with any other Co-Conspirator, FACEBOOK did not give any of the 50 million Americans notice that their User Information was taken by the other Co-Conspirators, and FACEBOOK did not remove the name and other personally identifying information from those 50 million Americans' information before the other Co-Conspirators took it.

Over 50 Million Americans are Victims of the Breach

34. As a result of FACEBOOK's negligent security practices, misrepresentations to its users, and delay in notifying affected consumers, these users are subject to an increased and real risk of identity theft based on the breach of their personal FACEBOOK information.

35. Affected users will have to spend time and money securing their User Information and protecting their identities. They will need to monitor their accounts and credit, and will have to pay for further identity theft protection services in the wake of the data breach, to make sure their identities were not stolen.

36. Now that their private User Information has been sold on the open market, consumers also face a real and immediate risk of identity theft and other problems associated with disclosure of this private information, and will need to monitor their credit and tax filings for an indefinite duration.

PLAINTIFF'S EXPERIENCE

37. At relevant times hereto, FACEBOOK collected and stored User Information from Plaintiff, including his biographical information, birthday, family and relationship status, what he was interested in, his religious and political views, his websites, whether he was online at any given time, any posts to his timeline, his hometown, his current location, his education

and work history, his activities, interests, and posts and pages he liked, and his activity in different apps.

38. Plaintiff has been a regular FACEBOOK user at all relevant times and has 1,050 Facebook friends. Plaintiff did not take the above-referenced fake personality quiz and did not ever consent to allowing GSR, SCL, or CAMBRIDGE to have access to his User Information. On information and belief, Plaintiff is one of the more than fifty (50) million Americans whose private User Information has been compromised by Co-Conspirator's actions.

39. Plaintiff did not know and could not know of the conduct alleged in this complaint until March 17, 2018, because Co-Conspirators, including FACEBOOK, never disclosed the breach to their victims.

40. As a result of the disclosure of his User Information to GSR, SCL and CAMBRIDGE and unknown others, Plaintiff has spent time and money securing his personal information and protecting his identity, by, for instance, purchasing identity theft protection. In addition, now that Plaintiff's information has been sold on the open market, Plaintiff faces a real and imminent risk of identity theft and other problems associated with disclosure of his private information, and will need to monitor his credit and tax filings for an indefinite duration.

CLASS ACTION ALLEGATIONS

41. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of himself and the following class:

> All persons in the United States whose personal data was stored by FACEBOOK and who had such data accessed by GSR, SCL, or CAMBRIDGE without authorization or in excess of authorization.

Excluded from the proposed class are anyone employed by counsel for Plaintiff in this action and any Judge to whom this case is assigned, as well as his or her staff and immediate family.

42. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy prerequisites for suing as a representative party pursuant to Rule 23.

43. Numerosity. The proposed class consists of over 50 million American consumers who had their data stolen by GSR, SCL and CAMBRIDGE through FACEBOOK making joinder of each individual class member impracticable.

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

44. Commonality. Common questions of law and fact exist for the proposed class' claims and predominate over questions affecting only individual class members.

Common questions include:

a. Whether FACEBOOK violated California Civil Code section 1798.81.5 by failing to implement reasonable security procedures and practices;

b. Whether FACEBOOK violated California Civil Code section 1798.82 by failing to promptly notify class members that their personal information had been compromised;

c. Whether FACEBOOK acted negligently in failing to maintain adequate security procedures and practices;

d. Whether FACEBOOK breached its contractual promises to adequately protect class members' personal information;

e. Whether FACEBOOK's failure to implement adequate security constitutes an unfair, unlawful, or deceptive practice under state consumer protection law;

f. Whether class members may obtain damages, restitution, declaratory and injunctive relief against FACEBOOK;

g. Whether class members had a reasonable expectation of privacy in the personal data and information they provided to FACEBOOK;

h. Whether GSR, SCL and CAMBRIDGE, by their actions, intentionally intruded into the class members' private and personal FACEBOOK data by mining it without their permission;

i. Whether GSR, SCL and CAMBRIDGE's intrusion was highly offensive to a reasonable person;

j. Whether class members were harmed;

k. Whether Co-Conspirator's conduct was a substantial factor in causing class members' harm;

l. Whether Co-Conspirators acts constitute a pattern of racketeering activity pursuant to 18 U.S.C. § 1961(5); and

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

m. What security procedures and data-breach notification procedure FACEBOOK should be required to implement as part of any injunctive relief ordered by the Court.

45. Typicality. Plaintiff's claims are typical of the claims of the proposed class because, among other things, Plaintiff and class members sustained similar injuries as a result of Defendants' uniform wrongful conduct and their legal claims all arise from the same core Defendants' practices.

46. Adequacy. Plaintiff will fairly and adequately protect the interests of the class. His interests do not conflict with class members' interests and he has retained counsel experienced in complex class action and data privacy litigation to vigorously prosecute this action on behalf of the class.

47. In addition to satisfying the prerequisites of Rule 23(a), Plaintiff satisfies the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual class members and a class action is superior to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing Defendants' conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

48. In addition, class certification is appropriate under Rule 23(b)(1) and/or (b)(2) because:

a. the prosecution of separate actions by the individual members of the proposed class would create a risk of inconsistent or varying adjudications which would establish incompatible standards of conduct for Defendants;

b. the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and

c. Defendants have acted or refused to act on grounds that apply generally to the proposed class, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed class as a whole.

FIRST CLAIM FOR RELIEF

For Violations of Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(c)

(Against Co-Conspirators)

49. Plaintiff incorporates the above allegations by reference.

50. The Political Deceit and Manipulation Enterprise is an enterprise engaged in, and whose activities affect, interstate commerce. This enterprise has been in operation since at least 2014.

51. On information and belief, Co-Conspirators agreed to and did conduct and participate, directly and indirectly, in the conduct of the Political Deceit and Manipulation Enterprise's affairs in a pattern of racketeering activity targeted at intentionally defrauding FACEBOOK users including, without limitation, via nominal payments and numerous intentionally false representations averred herein with the specific intent of inducing FACEBOOK users to unwittingly share other users' private User Information.

52. Pursuant to and in furtherance of their corrupt scheme, Co-Conspirators did in fact induce FACEBOOK users to unwittingly share other FACEBOOK users' User Information via hundreds of thousands of separate electronic monetary transfers.

53. Co-Conspirators willfully and knowingly devised a scheme with artifice to defraud FACEBOOK users and to obtain, sell, and use personal User Information by false pretenses and representations, including but not limited to the representation that the data would only be used for academic purposes.

54. The payments made or directed by CAMBRIDGE or SCL to GSR or any other entity to obtain FACEBOOK data were in furtherance of the fraudulent scheme. On information

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

and belief, those payments were made by wire transfer or other electronic means through interstate or foreign commerce.

55. The payments made from any Co-Conspirator or directed by any Co-Conspirator to takers of GSR's quiz were in furtherance of the fraudulent scheme. On information and belief, those payments were made by wire transfer or other electronic means through interstate or foreign commerce.

56. The acts of wire fraud averred herein constitute a pattern of racketeering activity pursuant to 18 U.S.C. § 1961(5).

57. The Co-Conspirators have directly and indirectly participated in the conduct of the Political Deceit and Manipulation Enterprise's affairs through the pattern of racketeering and activity alleged herein, in violation of 18 U.S.C. 1962(c). FACEBOOK aided and abetted the Co-Conspirators by misleading its users to believe that their data was safe, while permitting third-party apps like GSR's to access and use the data of non-consenting users without their permission and knowledge, and the other Co-Conspirators directly participated in the conspiracy by misleading quiz-takers that they were allowing Co-Conspirators' access to only their personal data for academic purposes, when in fact they were allowing access to their friends' data, and by fraudulently obtaining the data, selling it in interstate and foreign commerce, and using it to influence elections.

58. Plaintiff and class members were harmed by Co-Conspirators' conduct because the private information they did not intend to become public or disclose to third parties was acquired by companies who intended to and did use it illicitly for manipulating elections and other as yet unknown purposes. Furthermore, the security breach put Plaintiff and class members in imminent and real danger of having their identities stolen by anyone willing to pay these unscrupulous companies for the data. In addition, Plaintiff and class members spent time and money securing their personal information and protecting their identities, by, for instance, purchasing identity theft protection. The harm and value of the User Information is made plain by the fact that CAMBRIDGE paid $7 million to acquire the information.

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

59. As a direct and proximate result of Co-Conspirators' racketeering activities and violations of 18 U.S.C. § 1962(c), Plaintiff and the Class have been injured.

60. Plaintiff demands judgment in his favor against Co-Conspirators jointly and severally for compensatory, treble, and punitive damages with interest, the costs of suit and attorneys' fees, and other and further relief as this Court deems just and proper.

61. Co-Conspirators' acts as alleged herein were despicable and were carried out intentionally, with willful and conscious disregard of the rights or safety of Plaintiff and class members, subjecting them to cruel and unjust hardship. Co-Conspirators' conduct constitutes malice, fraud, and/or oppression, and Plaintiff and the class are therefore entitled to recover punitive and exemplary damages in an amount according to proof.

SECOND CLAIM FOR RELIEF

For Violation of the California Customer Records Act,

California Civil Code § 1798.80, *et seq.*

(Against FACEBOOK)

62. Plaintiff incorporates the above allegations by reference.

63. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted California Customer Records Act. This statute states that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Civil Code § 1798.81.5.

64. FACEBOOK is a "business" within the meaning of Civil Code § 1798.80(a).

65. Plaintiff and members of the class are "individual[s]" within the meaning of the Civil Code § 1798.80(d). Pursuant to Civil Code § 1798.80(e), "personal information" includes an individual's name, physical characteristics or description, address, telephone number, education, employment, employment history, and medical information.

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

66. The breach of the personal User Information of tens of millions of FACEBOOK customers constituted a "breach of the security system" of FACEBOOK pursuant to Civil Code § 1798.82(g).

67. By failing to implement reasonable measures to protect its customers' personal User Information, FACEBOOK violated Civil Code § 1798.81.5.

68. In addition, by failing to promptly notify all affected customers that their personal User Information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons, like GSR, SCL and CAMBRIDGE in the data breach, FACEBOOK violated Civil Code § 1798.82. FACEBOOK's failure to timely notify users of the breach has caused damage to class members who have had to buy identity protection services or take other measures to remediate the breach caused by FACEBOOK's negligence.

69. By violating Civil Code §§ 1798.81.5 and 1798.82, FACEBOOK "may be enjoined" under Civil Code § 1798.84(e).

70. Accordingly, Plaintiff requests that the Court enter an injunction requiring FACEBOOK to implement and maintain reasonable security procedures to protect customers' User Information in compliance with the California Customer Records Act, including, but not limited to: (1) ordering that FACEBOOK, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on FACEBOOK's systems on a periodic basis; (2) ordering that FACEBOOK engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that FACEBOOK audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that FACEBOOK, consistent with industry standard practices, conduct regular database scanning and securing checks; (5) ordering that FACEBOOK, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (6) ordering FACEBOOK to meaningfully educate its former and current users and employees about the threats they face as a result of the loss of their

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

personal User Information to third parties, as well as the steps they must take to protect themselves; and (7) ordering FACEBOOK to encrypt sensitive personal information.

71. Plaintiff further requests that the Court require FACEBOOK to (1) identify and notify all members of the class who have not yet been informed of the data breach; and (2) to notify affected former and current users and employees of any future data breaches by email within 24 hours of FACEBOOK's discovery of a breach or possible breach and by mail within 72 hours.

72. As a result of FACEBOOK's violation of Civil Code §§ 1798.81.5, and 1798.82, Plaintiff and members of the class have and will incur economic damages relating to time and money spent remedying the breach, including, but not limited to, monitoring their online presence to ensure that their identity has not been stolen or coopted for an illicit purpose, any unauthorized charges made on financial accounts, lack of access to funds while banks issue new cards, tax fraud, as well as the costs of credit monitoring and purchasing credit reports.

73. Plaintiff, individually and on behalf of the members of the Class, seeks all remedies available under Civil Code § 1798.84, including, but not limited to: (a) damages suffered by members of the class; and (b) equitable relief.

74. Plaintiff, individually and on behalf of the members of the Class, also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

THIRD CLAIM FOR RELIEF

Intrusion Upon Seclusion

(Against All Defendants)

75. Plaintiff incorporates the above allegations by reference.

76. Plaintiff and class members put User Information on their FACEBOOK profiles, including biographical information, birthdays, family and relationship status, their interests, religious and political views, websites, any posts on their or their friend's timelines, their hometown, their current location, their education and work history, their activities, interests, and posts and pages they liked, and their activity in different apps.

77. Importantly, Plaintiff and class members control – or at least were led to believe they control – via FACEBOOK's privacy settings, who has access to what information, be it private individuals, their FACEBOOK friends, the friends of their FACEBOOK friends, or the public at large. By putting their information on FACEBOOK, Plaintiff and class members expect to be able to control who may access that information and expect that only those individuals who they allow access to that information will be able to see it. As FACEBOOK puts it, Plaintiff and class members expect to "own all of [their] information." With respect to everyone else in the world, besides those who Plaintiff and class members give permission to see that information, their reasonable expectation is for that information to remain private.

78. By acquiring and using Plaintiff's and class members' data from their FACEBOOK accounts without their permission as alleged above, GSR, SCL and CAMBRIDGE intentionally intruded upon Plaintiff's and class members' private information.

79. FACEBOOK aided and abetted GSR, SCL and CAMBRIDGE's intrusion upon Plaintiff and class members' seclusion because it (1) knew or should have known about this intrusion; (2) gave substantial assistance to GSR, SCL and CAMBRIDGE by allowing apps like those used by GSR to access user's friends' User Information without their consent and not notifying their users of the breach or otherwise attempting to stop the breach or control the User Information leaked as a result of the breach for at least two years; (3) FACEBOOK's actions and failure to act was a substantial factor in causing harm to Plaintiff and class members because it had the capability of stopping the intrusion at any time, but knowingly failed to do so.

80. Defendants' intrusion and theft of Plaintiff's and class members' personal User Information from their FACEBOOK accounts was highly offensive to a reasonable person in that (1) GSR, SCL and CAMBRIDGE stole a huge amount of personal and private information about each person in order to effectively control and alter the votes of the American public; (2) GSR, SCL and CAMBRIDGE were motivated by profit and political ambition and their goal was to serve their owners' purposes of manipulating the American political process and preying on people's biases and tendencies to distort their beliefs and ultimately undermine American democracy; and (3) the intrusion occurred in the setting of FACEBOOK, a social media

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

company Americans trust – because of FACEBOOK's own representations – to take care of the data they share with their friends and family (and not with corporations attempting to fix elections through the use of misinformation).

81. Plaintiff and class members were harmed by Defendants' conduct because the private information they did not intend to become public was acquired by companies who intended to use it for the illicit purpose of manipulating elections. Furthermore, the security breach put Plaintiff and class members in imminent and real danger of having their identities stolen by anyone willing to pay these unscrupulous companies for the data. The harm and value of Plaintiff's and class members' User Information is also made plain by the fact that CAMBRIDGE paid $7 million to acquire the User Information. Plaintiff and members of the class have and will incur economic damages relating to time and money spent remedying the breach, including, but not limited to, monitoring their online presence to ensure that their identity has not been stolen or coopted for an illicit purpose, any unauthorized charges made on financial accounts, lack of access to funds while banks issue new cards, tax fraud, as well as the costs of credit monitoring and purchasing credit reports.

82. Defendants' acts as alleged herein were despicable and were carried out intentionally, with willful and conscious disregard of the rights or safety of Plaintiff and class members, subjecting them to cruel and unjust hardship. Defendants' conduct constitutes malice, fraud, and/or oppression, and Plaintiff and class members are therefore entitled to recover punitive and exemplary damages in an amount according to proof.

FOURTH CLAIM FOR RELIEF

For Unlawful and Unfair Business Practices Under

California Business and Professions Code § 17200, *et seq.*

(Against FACEBOOK)

83. Plaintiff incorporates the above allegations by reference.

84. FACEBOOK's acts and practices, as alleged in this complaint, constitute unlawful and unfair business practices, in violation of the Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq*.

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

85. The acts, omissions, and conduct of FACEBOOK also constitute a violation of the unlawful prong of the UCL because it failed to comport with a reasonable standard of care and public policy as reflected in statutes such as the Information Practices Act of 1977 and California Customer Records Act, which seek to protect individuals' data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

86. In failing to protect consumers' User Information and unduly delaying informing them of the data breach, while simultaneously misrepresenting to its consumers that the data was safe and would not be shared without their permission, FACEBOOK has engaged in unfair business practices by engaging in conduct that undermines or violates the stated policies underlying the California Customer Records Act and the Information Practices Act of 1977. In enacting the California Customer Records Act, the Legislature stated that: "[i]dentity theft is costly to the marketplace and to consumers" and that "victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative." 2002 Cal. Legis. Serv. Ch. 1054 (A.B. 700). FACEBOOK's conduct also undermines California public policy as reflected in other statutes such as the Information Practices Act of 1977, Cal. Civ. Code § 1798, et seq., which seeks to protect individuals' data and ensure that entities who solicit or are entrusted with personal data utilize reasonable security measures.

87. As a direct and proximate result of FACEBOOK's unlawful and unfair business practices as alleged herein, Plaintiff and members of the class have suffered injury in fact. Plaintiff and the class have been injured in that their personal information has been compromised and they are at an imminent risk for future identity theft and fraudulent activity. Plaintiff and class members have also lost money and property by purchasing credit monitoring services they would not otherwise had to but for FACEBOOK's unlawful and unfair conduct.

88. As a direct and proximate result of FACEBOOK's unlawful and unfair business practices as alleged herein, Plaintiff and class members face an increased risk of identity theft and medical fraud, based on the theft and disclosure of their personal User Information.

89. Because of FACEBOOK's unfair and unlawful business practices, Plaintiff and

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

the class are entitled to relief, including restitution to Plaintiff and class members for costs incurred associated with the data breach and disgorgement of all profits accruing to FACEBOOK because of its unlawful and unfair business practices, declaratory relief, and a permanent injunction enjoining FACEBOOK from its unlawful and unfair practices.

90. The injunctive relief that Plaintiff and members of the class are entitled to includes, but is not limited to: (1) ordering that FACEBOOK, consistent with industry standard practices, engage third party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on FACEBOOK's systems on a periodic basis; (2) ordering that FACEBOOK engage third party security auditors and internal personnel, consistent with industry standard practices, to run automated security monitoring; (3) ordering that FACEBOOK audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that FACEBOOK, consistent with industry standard practices, conduct regular database scanning and securing checks; (5) ordering that FACEBOOK, consistent with industry standard practices, periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; (6) ordering FACEBOOK to meaningfully educate its former and current users and employees about the threats they face as a result of the loss of their personal information to third parties, as well as the steps they must take to protect themselves; and (7) ordering FACEBOOK to encrypt sensitive personal information.

91. Plaintiff, individually and on behalf of the members of the class, also seeks reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

FIFTH CLAIM FOR RELIEF

Negligence

(Against FACEBOOK)

92. Plaintiff incorporates the above allegations by reference.

93. In collecting the User Information of its users, FACEBOOK owed Plaintiff and members of the class a duty to exercise reasonable care in safeguarding and protecting that User

Information. This duty included, among other things, maintaining and testing FACEBOOK's security systems and taking other reasonable security measures to protect and adequately secure the personal data of Plaintiff and the class from unauthorized access and use. FACEBOOK's security system and procedures for handling the personal User Information were intended to affect Plaintiff and the class. FACEBOOK was aware that by taking such sensitive information of users, it had a responsibility to take reasonable security measures to protect the data from being stolen and, in the event of theft, easily accessed.

94. The duty FACEBOOK owed to Plaintiff and members of the class to protect their personal User Information is also underscored by the California Customer Records Act.

95. Additionally, FACEBOOK had a duty to timely disclose to Plaintiff and members of the class that their personal User Information had been or was reasonably believed to have been compromised and made accessible to unauthorized third parties, like SCL and CAMBRIDGE. Timely disclosure is appropriate so that Plaintiff and members of the class could, among other things, monitor their online presence to ensure it has not been coopted for an illicit purpose, undertake appropriate measures to avoid unauthorized charges on their debit card or credit card accounts, purchase credit monitoring services, and change or cancel their debit or credit card PINs (personal identification numbers) to prevent or mitigate the risk of fraudulent cash withdrawals or unauthorized transactions.

96. There is a very close connection between FACEBOOK's failure to take reasonable security standards to protect its users' data and the injury to Plaintiff and the class. If not for FACEBOOK's negligence, GSR, SCL, and CAMBRIDGE would not have been able to steal Plaintiff's and the class's information and use it for their own political purposes.

97. FACEBOOK is morally to blame for not protecting the User Information, misrepresenting to its users how secure their User Information was, and by failing to take reasonable security measures. If FACEBOOK had taken reasonable security measures, data thieves, like GSR, SCL, and CAMBRIDGE would not have been able to take the personal User Information of over 50 million Americans and use it to manipulate the American people and undermine American democracy.

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

98. The policy of preventing future harm weighs in favor of finding a special relationship between FACEBOOK and the class. FACEBOOK's users count on FACEBOOK to keep their User Information safe and in fact are encouraged to share sensitive personal data with FACEBOOK. If companies are not held accountable for failing to take reasonable security measures to protect their customers' personal information, they will not take the steps that are necessary to protect against future data breaches.

99. It was foreseeable that if FACEBOOK did not take reasonable security measures, the User Information of Plaintiff and members of the class would be stolen. In fact, on information and belief, FACEBOOK was well aware that third-party apps like the one created by GSR could and did steal the User Information users who never consented to give those apps access to their information. Major corporations, particularly those in the social media industry, like FACEBOOK, face a higher threat of security breaches than other companies due in part to the large amounts and type of data they possess. FACEBOOK should have known to take precautions to secure its users' User Information, especially in light of the sheer volume of data accumulated by FACEBOOK from its users.

100. FACEBOOK breached its duty to exercise reasonable care in protecting the User Information of Plaintiff and the class by failing to implement and maintain adequate security measures to safeguard its users' User Information, failing to monitor its systems to identify suspicious activity or act on identified suspicious activity, allowing unauthorized access to the personal information of Plaintiff and the class, and failing to encrypt or otherwise prevent unauthorized reading of such User Information.

101. FACEBOOK breached its duty to timely notify Plaintiff and the class about the data breach. Additionally, FACEBOOK was, or should have been, aware of unauthorized access to its users' User Information as early as 2014.

102. But for FACEBOOK's failure to implement and maintain adequate security measures to protect its users' personal User Information and failure to monitor its systems to identify suspicious activity or act on identified suspicious activity, the User Information of

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

Plaintiff and members of the class would not have been stolen, and they would not be at a heightened risk of identity theft in the future.

103. FACEBOOK's negligence was a substantial factor in causing harm to Plaintiff and members of the class.

104. As a direct and proximate result of FACEBOOK's failure to exercise reasonable care and use commercially reasonable security measures, the User Information of current and former FACEBOOK users was accessed by unauthorized individuals who could use the information to commit identity fraud, medical fraud, or debit and credit card fraud. Plaintiff and the class face a heightened risk of identity theft in the future.

105. Plaintiff and members of the class have also suffered economic damages, including the purchase of credit monitoring services they would not have otherwise purchased.

106. Neither Plaintiff nor other members of the class contributed to the security breach, nor did they contribute to FACEBOOK's employment of insufficient security measures to safeguard User Information.

107. Plaintiff and the class seek compensatory damages and punitive damages with interest, the costs of suit and attorneys' fees, and other and further relief as this Court deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the proposed class, requests that the Court:

1. Certify this case as a class action on behalf of the class defined above, appoint Jonathan D. Rubin as class representative, and appoint Phillips, Erlewine, Given & Carlin LLP and Nicholas A. Carlin as class counsel;

2. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and other class members;

3. Award restitution and damages to Plaintiff and class members in an amount to be determined at trial;

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900

4. Award Plaintiff and class members their reasonable litigation expenses, costs, and attorneys' fees;

5. Award Plaintiff and class members treble damages under 18 U.S.C. § 1964(c);

6. Award Plaintiff and class members pre- and post-judgment interest, to the extent allowable; and

7. Award such other and further relief as equity and justice may require.

Dated: March 26, 2018

PHILLIPS, ERLEWIN, GIVEN & CARLIN LLP

By: /s/ Nicholas A. Carlin
Nicholas A. Carlin
Brian S. Conlon
Attorneys for Plaintiff

JURY DEMAND

Plaintiff hereby demands a jury trial on all issues so triable.

Dated: March 26, 2018

PHILLIPS, ERLEWIN, GIVEN & CARLIN LLP

By: /s/ Nicholas A. Carlin
Nicholas A. Carlin
Brian S. Conlon
Attorneys for Plaintiff

PHILLIPS, ERLEWINE, GIVEN & CARLIN LLP
39 Mesa Street, Suite 201 – The Presidio
San Francisco, CA 94129
Telephone: (415) 398-0900